THIRD PARTY RISK

CAPCO

INTRODUCTION

Financial institutions continue to find efficiencies in outsourcing an ever-expanding number of services to outside parties. For many institutions, establishing these third-party relationships may be the only reasonable way a company can engage in certain activities to help accomplish strategic corporate initiatives and meet customer demands. Whether the third-party offers products that can be sold to the company's customers or provides services, such as payment processing or call center support, institutions of all sizes can gain competitive advantages in the marketplace by utilizing service providers.

THIRD-PARTY RELATIONSHIPS

It is important to understand the difference between the following three variations of third-party relationships and how institutions may use may utilize these outside resources.

Co-sourcing

In co-sourcing, the institution keeps certain aspects of the task in house and uses a third party for the remaining parts of the task.

Partnering

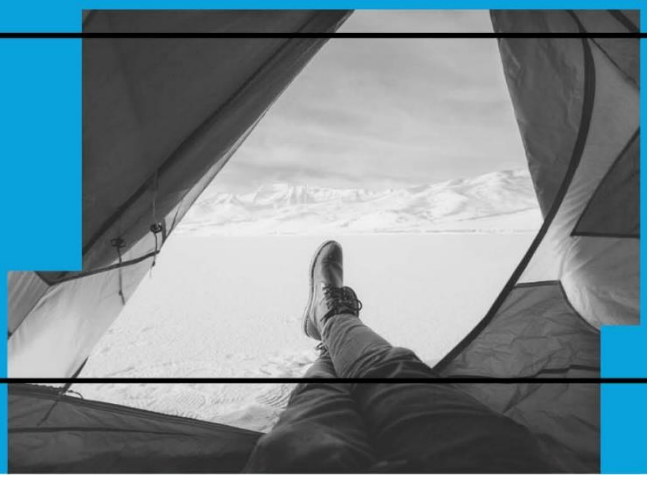
With partnering, the institution is fully in charge, but utilizes specialized and highly skilled resources to perform certain tasks that are difficult to manage or staff in-house.

Outsourcing

In general, outsourcing means the institution hands off the entire task to the third party and relies on the third party for all aspects of delivery.

The extent to which an institution gives a third party control and responsibility to undertake a task increases (**outsourcing**), hands-on oversight and ownership of risk management will typically decrease. On the other end of the spectrum, the extent to which a third party is given control and responsibility to undertake a task decreases (**partnering),** hands-on oversight and ownership of risk management will typically increase.

THIRD PARTY RISK



CAPCO

EMERGING RISKS AND EFFECTIVE MITIGATION STRATEGIES

Trending areas of focus for emerging third-party risk include six major areas within institutions.

Cybersecurity

Entering a third-party relationship forces an institution to give up a certain level of control over the product, service or process being delegated to the third party. In the financial services industry, this is most notable when a third party requires access to sensitive information to complete its contractual duties. Financial institutions may have strong internal controls and comprehensive policies and procedures for providing preventative and monitoring controls to address cyberthreats; however, management may not always apply the same security guidelines when contracting a third-party service provider. A key to maintaining accountability and responsibility for third-party cybersecurity controls is to ensure that the institution has included the appropriate contractual obligations and protections through comprehensive service agreements.

Payment Card Industry (PCI) Standards

Connection with the payment card industry (PCI) poses an additional layer of risk for financial institutions and presents many opportunities for interconnectivity with other players in the market. For institutions connected to the payment card industry, resources are likely dedicated to maintaining certification with the payment card brands represented by the Payment Card Industry Security Standards Council (PCI-SSC). Embedded within these, institutions will find requirements that directly implicate some of the third-party relationships. Perhaps most obvious is the part of requirement 12.2 of the PCI requirements, which mandates completion of a risk assessment. This should include an assessment of third-party service providers. An efficient risk assessment will help ensure that third-party oversight is risk-based and that a company remains most vigilant regarding the third parties that pose the highest risks to the organization. It also allows ongoing tracking of critical information for each third-party service provider.

Business Resiliency

The Federal Financial Institutions Examination Council's (FFIEC) Appendix J, Strengthening the Resilience of Outsourced Technology Services, provides a framework for financial institutions when using third-party service providers for critical processing services. The guidance helps ensure that adequate business resiliency is accomplished through:

Third-Party Management
Standard risk management activities, including due diligence, regular monitoring and strategic alignment with third-party service providers;

Third-Party Capacity
Ability of third parties to deliver essential services under adverse disaster scenarios and considerations for alternatives in the event of third-party failure;

Testing with Third-Party Technology Service Providers
Testing the business continuity resilience among the financial institution and third-party service providers and reviewing the test results and remediation of any observed weaknesses. Obtain the third party's business continuity testing results to ensure that the institution's recovery time objectives (RTOs) can be attained; and

Cyber Resilience
Identify and mitigate cyberthreats to data and operational infrastructure and maintain effective incident response procedures to cyberattacks.

Subcontractors

It is not uncommon to see third parties subcontract out certain tasks. Responsibilities and liabilities should be clearly outlined, and subcontractors should be held to the same data security, confidentiality and non-disclosure agreement standards as the contracted third party. It is incumbent on the institution to ensure that its third parties can demonstrate a credible third-party oversight program themselves. Otherwise, the company may be expected to provide direct oversight regarding these fourth parties as well. A lack of adequate control over subcontractor activities will significantly increase third-party risk.

THIRD PARTY RISK

CAPCO

Regulatory Risks

Proactive management of third-party relationships can help mitigate risks associated with specific laws and regulations. An example of regulatory risks associated with common third parties are those under the Fair Debt Collections Practices Act (FDCPA) for outsourced collections and under the Fair Credit Reporting Act (FCRA) for interactions with consumer reporting agencies. A key high-risk area that institutions should also consider, especially where the third party interacts directly with consumers, is the prohibition on unfair, deceptive or abusive acts or practices (UDAAPs). The Consumer Financial Protection Bureau (CFPB) Supervision and Examination Manual also reminds institutions that anything a third party does to threaten a consumer's financial well-being will ultimately become a problem for the institution. Another aspect to consider is if the third party has aligned its controls with the expectations and risk appetite of the institution. This includes a review of the third party's compliance management system (CMS) for adequate policies and procedures, risk assessment, training, compliance audits, monitoring and other appropriate controls for ensuring compliance.

Terminating the Relationship

As part of the institution's third-party risk management program, an institution should develop policies and procedures addressing third-party relationship termination strategies to ensure that the termination is managed appropriately. An effective termination or exit strategy will help to identify and address possible risks, define potential losses and ensure continuity of services.

The institution's third-party relationship managers and owners should actively track and manage contracts and service agreements with third parties. Contractual provisions for termination often vary with the type of service provider. Monitoring provisions should be part of an ongoing review process. At minimum, it is helpful to monitor the following items;

- Contract term
- Contract expiration date
- Non-Renewal notification days
- Automatic renewal terms
- Obligations after termination
- conditions for breach or default of contract
- Terms and conditions for early termination

KEY TAKE-AWAYS

- Develop a compliance training program that carves out resources to ensure third parties are properly trained on all relevant compliance topics.
- Require the service provider to include provisions in its contracts with subcontractors that allow the institution to audit or access the institution's data and information in possession of the subcontractor.
- Ensure that the complaint management program evaluates complaints directly against the third party, as well as against the institution, that stem from third-party activities.
- Request information from the third party on its own complaint management process and regularly review complaints logged by the third party, including how it responded.

For more information on third-party risk, email us at cri.capco@capco.com